CLAIMS

What is claimed is:

1. A method of performing electronic communications between members of a group wherein the communications are authenticated as being from a member of the group and have not been altered, the method comprising the steps of:

generating a plurality of random numbers;

distributing in a digital medium the plurality of random numbers to the members of the group;

publishing a hash value of contents of the digital medium;

distributing to the members of the group public-key-encrypted messages each containing a same token comprising a random number; and

encrypting a message with a key generated from the token and the plurality of random numbers.

2. The method of claim 1 wherein the generating step comprises generating at least approximately 20,000 random numbers.

3. The method of claim 2 wherein the generating step comprises generating 256-bit random numbers.

4. The method of claim 1 wherein the step of distributing in a digital medium comprises distributing in a removable digital medium.

5. The method of claim 4 wherein the step of distributing in a digital medium comprises distributing in a medium selected from the group consisting of CD-ROMs and DVD-ROMs.

6. The method of claim 1 wherein the steps of publishing a hash value comprises employing a Secure Hash Algorithm.

7. The method of claim 1 additionally comprising the step of rejecting a digital medium received by a user if a hash value of contents of the received digital medium does not equal the published hash value of the contents of the distributed digital medium.

8. The method of claim 1 wherein the step of distributing a token is performed daily.

9. The method of claim 1 wherein the step of distributing a token comprises distributing a verification message comprising an element for each user, each element comprising the token encrypted with the corresponding user's public key, and the method additionally comprises the step of publishing a hash value of the verification message.

10. The method of claim 9 additionally comprising the step of rejecting a token received by a user if a hash value of a received verification message does not equal the published hash value of the distributed verification message.

11. The method of claim 10 additionally comprising the step of rejecting a token received by a user if every element of the verification message does not equal the received token encrypted with the corresponding user's public key.

12. The method of claim 1 wherein the encrypting step comprises employing symmetric key encryption.

13. The method of claim 1 wherein the encrypting step comprises choosing randomly one of the plurality of random numbers.

14. The method of claim 13 additionally comprising the step of sending the encrypted message with an index to the randomly chosen number and a timestamp sufficient to enable a recipient to determine a proper decryption token.

15. The method of claim 1 wherein the group is a domain.

16. The method of claim 1 wherein one or more members of the group is a domain.

17. The method of claim 1 wherein anonymity of a sender of the message is maintained.

18. The method of claim 17 additionally comprising the step causing the encrypted message to be transmitted over a network such that a recipient of the encrypted message receives no data concerning network routing of the encrypted message.

19. The method of claim 18 wherein the step causing the encrypted message to be transmitted over a network comprises employing onion routers.

20. The method of claim 19 wherein employing onion routers comprises encrypting messages received by the onion routers with a public key of the recipient.

21. The method of claim 1 wherein the method provides absolute anonymity for communications between the members.

22. The method of claim 21 wherein the method provides absolute anonymity as to authorship of the communications and as to electronic mail routing of the communications.

23. The method of claim 1 wherein the method provides relative anonymity for communications between the members.

24. The method of claim 23 wherein anonymity is not provided for communications between members of the group within a same domain.

25. A method of performing anonymous electronic communications between members of a group wherein the communications are authenticated as being from a member of the group and have not been altered, the method comprising the steps of:

generating a plurality of random numbers;

distributing in a digital medium the plurality of random numbers to the members of the group; and

encrypting a message with a key generated from a token and the plurality of random numbers while maintaining anonymity of authorship of the message.

26. A method of performing anonymous electronic communications between members of a group wherein the communications are authenticated as being from a member of the group and have not been altered, but wherein said communications are revocable, the method comprising the steps of:

generating a plurality of random numbers;

distributing in a digital medium the plurality of random numbers to the members of the group;

encrypting a message with a key generated from a token and the plurality of random numbers; and

permitting revocation of the message by a revocation authority comprising one or more of the members.

27. The method of claim 26 wherein the permitting step maintains anonymity of authorship of the message.